2021-04-23 R&S 2.0 Notes

Attendees

- Pål Axelsson
- Björn Mattsson
- Scott Cantor
- Miroslav Milinovi
- Heather Flanagan
- Andrew Morgan
- Alan Buxey
- Jií Pavlík
- Jens Jensen - STFC UKRI
- Alex Stuart
- Jon Agland

Working Draft

- Draft spec for R&S 2.0

Agenda

1. Recap of consensus so far - **note that all changes will need to be validated via the consultation process**
    a. The FAQ will be revised to offer clarity on the term "affiliation" (see Research and Scholarship FAQ) and editorial changes made to the spec to make it more clear (see new draft spec for updated structure)
    b. eduPersonScopedAffiliation will become a required value
    c. R&S will require privacy statements
    d. subject-id should be listed as the new identifier
    e. R&S 1.3 and R&S 2.0 can co-exist; no migration detail will be included in the spec itself.
    f. ePPN and targeted ID to both be removed from R&S 2.0
    g. Information on OIDC requirements will be moved to R&S 2.1 (after the OIDF OIDCre working group has formal documentation in this space)
    h. eduPersonAssurance will be required, RAF recommended
2. Home Organization use case, continued
    a. introducing schacHomeOrg to R&S (which will be a lift since SCHAC isn't globally used), or adding a value to eduPersonScopedAffliation (which has its own lift)
    b. need clarity on the complex use cases (or real-world examples) to help describe what the IdP would assert when the IdP has several different organizations involved
3. Proposal to require DisplayName (Petersen)

Notes

1. Recap of consensus so far - **note that all changes will need to be validated via the consultation process**
    a. The FAQ will be revised to offer clarity on the term "affiliation" (see Research and Scholarship FAQ) and editorial changes made to the spec to make it more clear (see new draft spec for updated structure)
    b. eduPersonScopedAffiliation will become a required value
    c. R&S will require privacy statements
    d. subject-id should be listed as the new identifier
    e. R&S 1.3 and R&S 2.0 can co-exist; no migration detail will be included in the spec itself.
    f. ePPN and targeted ID to both be removed from R&S 2.0
    g. Information on OIDC requirements will be moved to R&S 2.1 (after the OIDF OIDCre working group has formal documentation in this space)
    h. eduPersonAssurance will be required, RAF recommended
2. Home Organization use case, continued
    a. introducing schacHomeOrg to R&S (which will be a lift since SCHAC isn't globally used), or adding a value to eduPersonScopedAffliation (which has its own lift) - POLL
    b. need clarity on the complex use cases (or real-world examples) to help describe what the IdP would assert when the IdP has several different organizations involved
        i. Miro and Christos did not have time to write this up. The use case we had talked about was the mobility use case.
        ii. One case to argue for is a proxied scenario where an IdP is fronting several organizations (e.g., a proxy or a hub-and-spoke federation). If you don't assume they are asserting attributes that would mask the proxy, you could do that by making the proxy a detail where it would not be asserting affiliations in the proxy's namespace. Instead, they would add information from whatever organizations they are proxying. This isn't spelled out anywhere as a rule or even best practice guidance. In this proxy use case, in order to do that would need an attribute to carry this information. We could write language in the spec that this isn't expected to be supported within R&S.
        iii. It may be that this is really too specific for R&S. How globally would this be used? Can we add this requirement when it will not be used out of this specific, European use case?

iv. The AARC community is very interested in ways to use ScopedAffiliation. There is a gap in the available required values; a gap that might impact this use case is that if someone doesn't qualify as a member, then there is no way to indicate another relationship to the organization. Should an IdP allow an authentication to proceed if it can't assert any eduPersonScopedAffiliation value? It is valid because R&S doesn't have to be universal, but we also need more text about this. We will need to say something somewhere about what to do if there is no affiliation with the institution when asserting something in eduPersonScopedAffiliation.
v. As a service provide, I need to have a way to verify that the user has a relationship with the institution. Does a visiting individual (guest) count as any kind of member to the organization?
vi. If a hub-and-spoke org asserts "student@hub" and not "student@university" that would be a problem for this use case. If we can say that the scope of eduPersonScopedAffiliation is the home organization, then we can use this.
vii. Interesting reading
    1. AARC G025 on expressing affiliation https://docs.google.com/document/d/15eK80-h9SwPka0EYhbpI3QwJIW2Bt-URkf0jfIeuinY/edit?usp=sharing
    2. AARC Guidelines on expressing group membership and role information may be useful as well. https://aarc-project.eu/wp-content/uploads/2017/11/AARC-JRA1.4A-201710.pdf
viii. Poll: How should we handle the need for home organization in R&S 2.0? Require schacHomeOrg - 0%; Add guidance for the use for eduPersonScopedAffiliation - 90%; Do nothing (don't try to support this use case in R&S) 10%; Need more information - 0%
ix. We will need more information on what guidance we want to offer here; the guidance in the spec should describe what to do in the use case when using this attribute. Scott will propose text in the draft.

3. Proposal to require DisplayName (Peter S) - POLL
    a. There is a functional reason why DisplayName and the other names are different. The DisplayName was the more generally useful case.
    b. What to do if there is only one name? What should an institution use if they have no value for a part of the name? We need to offer guidance if we start requiring this.
    c. We'll need to remind people that "required" means it's present when it can be, but if there is no value (e.g., no givenname) then that's valid. There is concern that SPs will be making decisions to split on whitespace whatever is provided in DisplayName, which may be bad.
    d. Poll: Should R&S 2.0 require DisplayName AND require given/sn? Yes, DisplayName and Given/SN should all be required - 60%; No, they should be left as is (optional) - 0%, It should only require DisplayName, with Given/sn as optional - 30%; I need more information - 10%
    e. We'll update the draft to require DisplayName and givenname/sn, and we'll see what comes out of the consultation. Note that we're not trying to drive SPs to any particular behavior here; we're trying to given them what's most commonly useful, respecting cultural impertatives.